Securing Our Ports

America's seaports remain vulnerable to terrorist attacks. Terrorists could cause mass casualties and serious damage to the economy if a weapon of mass destruction (WMD) is detonated in a container or if a large passenger vessel is attacked. The Department of Homeland Security has several initiatives dedicated to preventing terrorists from attacking America's ports. Despite these efforts, many security gaps remain. Container shipments are not secure from their points of origin to their final destination, and many ports are struggling to make physical security improvements. To remedy these problems, the Administration should improve the integrity of container shipments, develop a credible system of inspection and make sufficient resources available to local ports for security enhancements.

America's maritime transportation system is the gateway to the global economy. Our country's economic prosperity rests on the ability of tons of containerized cargo arriving unimpeded at U.S. ports to support the "just-in-time" delivery system, that underpins our manufacturing and retailing sectors. A majority of America's energy sources arrive in large oil and gas tankers. America's ports and waterways are also used to carry millions of citizens on cruise ships and ferries. While the transportation system is incredibly efficient, as port security expert Stephen Flynn states "it was built without credible safeguards to prevent it from being exploited or targeted by terrorists or criminals."[1] An attack in a port could result in a substantial loss of life and an economic damage ranging from $58 billion to $1 trillion.[2]

There are many vulnerabilities within the maritime transportation system. The high volume of containers and their efficient movement from foreign ports to the U.S. make container shipments a prime target for terrorist activity. Cargo containers could be used to smuggle terrorists or dangerous materials into the U.S. or as the delivery vehicle for a weapon of mass destruction. The Intelligence Community has warned that the United States is more likely to be attacked with a weapon of mass destruction delivered by ship, truck, or airplane than by a ballistic missile.[3] Large fuel tankers, cruise ships, and ferries are vulnerable to a variety of threats ranging from an explosive device being placed on board or small boat attacks similar to those on the *USS Cole* or French tanker *Limberg.* Such attacks could have significant fatalities, cause serious environmental damage, or potentially block the entranceway to a harbor, bringing local commerce to a halt. The Interagency Commission on Crime and Security at Seaports concluded just prior to 9/11 that security at U.S. ports "generally ranges from poor to fair and in few cases good."[4]

---

[1] Council on Foreign Relations, Testimony of CDR Stephen Flynn, USCG (ret), Jeane J. Kirkpatrick Senior Fellow in National Security Studies,*The Fragile State of Container Security*, Stephen Flynn, before the Committee on Governmental Affairs, United States Senate, Stephen Flynn (Washington D.C.: March 20,2003)

[2] $58 billion estimate is from the *Port Security Wargame-Implications from the Supply Chain*, Booz-Allen-Hamilton. February 2003. www.boozallenhamilton.com. $1 trillion comes from Michael O' Hanlon, *Protecting the American Homeland*, (Washington D.C.:The Brookings Institute Press 2002.)

[3] U.S. National Intelligence Council, *Foreign Missile Developments and the Ballistic Missile Threat Through 2015*, December 2001. www.cia.gov/nic/other_missilethreat2001.html

[4] Interagency Commission on Crime and Security at U.S. Seaports, Fall 2000, 5.

Container Security

Improving container security is a major challenge. Individual containers must be made less vulnerable to tampering, and companies must strengthen the security of their supply chains. Finally, the inspections process must be made more vigorous without imposing an undue burden on the flow of commerce.

SECURITY GAP: Cargo Containers Are Vulnerable to Tampering.

One of the major vulnerabilities of container shipments is the lack of physical security of containers as they transit through the supply chain. The physical security of containers has long been a problem as criminals have easily broken into them to steal cargo and smuggle contraband. According to a recent RAND report on container security, there are no minimum security standards for containers.[5] The majority of containers are sealed with a lead tag which does not prevent access into a container. In addition, criminals break into containers without disturbing the seals such as cutting into the side or removing the doors.[6] According to RAND, an experienced thief can break into a sealed container in twenty minutes without disturbing the seals.[7]

The Administration has undertaken a series of efforts to address the problem through initiatives such as Operation Safe Commerce and the Smart Box Initiative. Operation Safe Commerce is a demonstration program managed by the Transportation Security Agency (TSA) that has attempted to identify technology to secure containers such as electronic seals that signal an alarm if tampering occurs. It will expire at the end of fiscal year 2004. The Smart Box Initiative is a Customs and Border Protection (CBP) program, in which aims to reward companies that seal containers with a security seal and place sensors inside their containers by reducing the likelihood these containers would be delayed in the inspection process. While these efforts are admirable, the end result is that DHS still has not developed minimum standards for sealing containers. Rather, DHS has recently announced that it will be working with industry over the next six months to develop "recommendations" for sealing requirements. Thus for the foreseeable future, millions of containers will continue arriving in the U.S. sealed with tags that are not tamperproof.

In addition to the physical security weaknesses of containers, there is no process for verifying that containers remain sealed as they move through the supply chain. A container moves through many port terminals between the time it is loaded at a warehouse and when it reaches its final destination. This gives terrorists many opportunities to break into a container, plant a weapon of mass destruction inside and reseal it without anyone checking to see if the container has been opened until it reaches a U.S. port.

---

[5] Voort, Maarten van de, Kevin O'Brien, Adman Rahman, and Lorenzo Valeri. *Seacurity: Improving the Security of the Global Sea-Container Shipping System*, (RAND) August 12, 2003, 9.

[6] Council on Foreign Relations, Testimony of CDR Stephen Flynn, USCG (ret), Jeane J. Kirkpatrick Senior Fellow in National Security Studies,*The Fragile State of Container Security*, Stephen Flynn, before the Committee on Governmental Affairs, United States Senate, Stephen Flynn (Washington D.C.: March 20,2003)

[7] Voort, Maarten van de, Kevin O'Brien, Adman Rahman, and Lorenzo Valeri. *Seacurity: Improving the Security of the Global Sea-Container Shipping System*, (RAND) August 12, 2003, 9.

SECURITY RECOMMENDATION

Container integrity can be enhanced through the adoption of minimum standards for container seals and the development of a seal verification process. DHS, at a minimum, should require all shippers to seal containers with the high security seal approved by the International Standards Organization. This is an electronic or mechanical seal that has unique markings and easily shows signs of tampering compared to lead tags seals currently in use. DHS also should develop a chain of custody for containers, requiring the verification of seals at the major stages of the supply chain such as when a container is loaded, or when placed on a vessel, train, or truck. Radio Frequency Identification technology can play a helpful role in verifying the status of seals.

SECURITY GAP: Containers Traveling Through the Supply Chain Are Vulnerable.

Containers are very susceptible to terrorist exploitation as they move through the supply chain. Many foreign warehouses do not have solid security controls including criminal background checks on personnel. The transit between the warehouse and foreign departure ports is believed to highly vulnerable, as containers carried on trucks and trains sit unguarded in parking lots, loading docks, and rail yards. While security at most foreign ports is a better than security at warehouses, many foreign ports have not yet taken the steps to improve their security in accordance with the International Maritime Organization port security requirements.[8] Containers placed on ocean carriers may not be sealed or checked for tampering. Once a container vessel arrives in the U.S., it is loaded on a truck or train and taken to its final destination. During this phase the whereabouts of the cargo are unknown, creating a vulnerability similar to the transit between the warehouse and foreign port.

The DHS developed the Customs Trade Partnership Against Terrorism (C-TPAT) to strengthen supply chain security. Launched in November 2001, C-TPAT is a government-business initiative between CBP and industry designed to improve security by having companies volunteer to sign agreements committing them to implementing a set of security practices in their supply chain. In return, participating companies have their score in CBP's Automated Targeting System (ATS) lowered, reducing the likelihood their shipments will be inspected. DHS officials have boasted about the success of C-TPAT. In October 2003, CBP Commissioner Robert Bonner stated that "C-TPAT is the largest and most successful government-private sector partnership to emerge from the ashes of 9-11."[9]

C-TPAT is a useful first step in encouraging the private sector in being pro-active about supply chain security. However, C-TPAT's potential is being compromised by CBP's limited resources to process the applications of 5,300 companies and to conduct on-site verification of the

---

[8] Mark Huband,"Terrorist Threat to Shipping Still High as Authorities Slow to Implement Security Code. *Financial Times*, November 17, 2003, 13. The International Maritime Organization develop The International Ship and Port Facility Security (ISPS) code in December 2002. 163 nations included the US are signatories.

[9] U.S. Bureau of Customs and Border Protection, Remarks by Commissioner Robert Bonner, C-TPAT Conference, October 30, 2003.
http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/oct302003.xml

companies' security practices.[10] According to Stephen Flynn, the major weakness in C-TPAT is "the nearly complete absence of Customs personnel to monitor the level of compliance among C-TPAT participants."[11] Although CPB is currently conducting validations, it does not have enough personnel to complete them within the next year. This fact is troubling in light of the threefold increase in C-TPAT membership over the last year. As of January 2004, only 130 C-TPAT members had been verified leaving thousands of companies receiving a benefit of reduced inspections without any assurance that security has actually improved.[12] CBP requested an additional $15.2 million in its fiscal year 2005 budget to hire 120 supply chain specialists to conduct validations. These positions will be combined with new personnel expected to be hired in 2004 as a result of resources previously provided by Congress. However, given the growth of the program such resources may not be sufficient to ensure that all companies can have their security practices validated within the next year. CBP also does not have a plan to audit C-TPAT members at a regular interval after they have received initial validation or conduct random inspections to ensure they comply with C-TPAT guidelines. Another weakness, according to RAND, is that C-TPAT does not address the land transit of containers to foreign debarkation ports, which it describes as the "most vulnerable phase in a container's transport."[13]

SECURITY RECOMMENDATION

CPB should improve its ability to validate C-TPAT companies to ensure they are not receiving the benefit of reduced inspections without meeting their security responsibilities. CBP should strive to complete the validations within the next year. One possible solution is a partnership with reputable private companies to conduct the on-site verifications. These private companies would model the classification societies used in marine safety which are recognized by the U.S. Coast Guard to ensure vessels comply with international safety standards. These companies would be subject to CBP oversight. An annual audit plan should be developed to ensure that companies' security practices are checked beyond the final validation. CBP should establish "red teams" to test security compliance beyond announced examinations and determine whether C-TPAT security measures are sound.

---

[10] Bureau of Customs and Border Protection, Testimony of Robert Jacksta, Executive Director Border Security and Facilitation Office of Field Operations, Before Committee on the Juidiciary, United States Senate, January 27, 2004.

[11] Council on Foreign Relations, Testimony of CDR Stephen Flynn, USCG (ret), Jeane J. Kirkpatrick Senior Fellow in National Security Studies,*The Fragile State of Container Security*, Stephen Flynn, before the Committee on Governmental Affairs, United States Senate, Stephen Flynn (Washington D.C.: March 20,2003)

[12] Bureau of Customs and Border Protection, Testimony of Commissioner Robert Bonner, Before the National Commission on Terrorist Attacks Upon the United States. January 26, 2004. http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/jan262004.xml

[13] Voort, Maarten van de, Kevin O'Brien, Adman Rahman, and Lorenzo Valeri. *Seacurity: Improving the Security of the Global Sea-Container Shipping System*, (RAND) August 12, 2003, 4.

SECURITY GAP: Container Inspections Are Not Sufficiently Comprehensive To Detect or Deter Attacks.

Recognizing that a nuclear weapon smuggled in a cargo container is one of the most significant threat facing America, DHS has attempted to improve the process used to inspect cargo. Prior to 9/11, the former Customs Service inspected two percent of all cargo containers by physically opening them to verify the contents. After 9/11, security officials acknowledged that the threat of chemical, biological or nuclear weapons being smuggled into the U.S. in a container required such containers to receive greater scrutiny. However, with more than seven million containers arriving at U.S. seaports annually, government officials realized that physically searching 100 percent of containers would be impractical and would severely slow down the flow of commerce. In response, DHS developed a risk management approach to identify high risk containers that warrant further scrutiny. CBP has created a cargo targeting center, required freight manifest information be submitted 24-hours prior to loading, assigned inspectors overseas, required the inspection of all high risk containers and placed some non-intrusive inspection equipment at U.S seaports.

Such efforts, however, are not sufficient to ensure that the current inspection regime is an effective deterrent. Even with the previously mentioned improvements, CBP still inspects, either through physical inspection or some technological screening, only five percent of inbound containers. Furthermore, a technical recent report completed by Professor Lawrence Wein of Stanford University and Stephen Flynn concluded that current inspection practices have a only ten percent likelihood of detecting the most significant threat, a shielded nuclear weapon smuggled in a container.[14]

- **Targeting Efforts Require Improvement to Determine Which Containers Pose a Risk.**

The National Targeting Center (NTC) is an operation center that is run by CBP responsible for reviewing manifest data in the ATS to determine which container shipments should be inspected. The NTC sets the anti-terrorism parameters for ATS and sends targeting information to inspectors at foreign and U.S. seaports. CBP also has manifest review units that are responsible for targeting containers headed to U.S. ports. The NTC's efforts are helped by the 24-hour rule, which requires carriers to send CBP manifest data 24 hours before a container is loaded on a vessel. The rule also requires specific information about the cargo which is an improvement over the vague cargo descriptions provided by shippers before 9/11.

Even with these improvements container targeting is flawed. The major weakness is that the data used by the NTC and CBP inspectors primarily comes from cargo manifests. According to GAO testimony on targeting, manifests are recognized by terrorism experts, the trade community, and CBP inspectors to be unreliable documents for targeting purposes. [15] If the data inputted into ATS is flawed, then the risk assessment of a container is unreliable and the entire container inspection system is suspect. Another problem with CBP targeting is that shippers are allowed

---

[14] Lawrence Wein, Alex Wilkins, Manas Baveja, and Stephen Flynn, *Preventing the Importation of Illicit Nuclear Materials in Shipping Containers*. November 4, 2003.

[15] Richard Stanna, *Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers*. U.S. General Accounting Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. December 16, 2003, 11.

revise manifests sixty days after a container arrives. According to GAO, one-third of the manifest revisions resulted in a higher ATS score, but by the time the revisions were discovered, the cargo often was inside the U.S. after having been released from its arrival port.[16]

SECURITY RECOMMENDATION

CBP must strengthen its targeting system by requiring the submission additional trade information which includes a more specific description of the cargo verified by the exporter and reduce the time period in which information on a manifest can be changed. DHS should develop a system to share threat and vulnerability information with all of the industries in the supply chain. This system could exist in the form of an Information Sharing and Analysis Center (ISAC) used in other industries. Ports, carriers, and shippers could report on security lapses in the supply chain to the ISAC and in return would have access to unclassified maritime threat and security information such as piracy incidents. This system would greatly help CBP's targeting efforts because it will give targeting personnel specific information on supply chain security breakdowns which does not exist in trade data.

- **Cargo Containers Are Not Comprehensively Screened For Weapons of Mass Destruction.**

According to CBP, it is addressing the weapons of mass destruction threat by deploying non-intrusive inspection devices such as radiation pagers, handheld isotope identifiers and Vehicle and Cargo inspection (VACIS) machines at seaports. Despite CBP Commissioner Bonner's continued statement that radiation pagers are "an important tool to detect radioactive materials moving through a port" the radiation pagers are a safety device that alarm inspectors of the presence of radiation.[17] Officials at the Department of Energy have stated that the pagers are not are not search instruments and are not designed to detect weapons usable nuclear material such as enriched uranium.[18] The handheld isotope identifiers can identify the type of radiological or nuclear material that may be in a container, but are primarily used as a secondary inspection device. VACIS is primarily an x-ray machine, providing an image of the contents inside a container but these machines are not capable of detecting radiological or nuclear material. In addition, many ports only have one VACIS machine, which is insufficient to screen all high risk containers at many seaports. CBP did not request any additional VACIS machines for domestic ports in its fiscal year 2005 budget.

Radiation portal monitors are the non-intrusive detection devices most capable of detecting nuclear and radiological material. The other great advantage of radiation portals is they can be fully integrated into port operations, which means that containers can be run through a portal by truck and rail without slowing the movement of commerce. Thus, not only are these portals far

[16] Ibid.

[17] Bureau of Customs and Border Protection, Testimony of Commissioner Robert Bonner, Before the National Commission on Terrorist Attacks Upon the United States. January 26, 2004. http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/jan262004.xml

[18] Gary L. Jones, *Customs Service: Acquisition and Deployment of Radiation Detection Equipment.* U.S. General Accounting Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. October 17, 2002.

superior to pagers and VACIS machines for the purpose of identifying dangerous materials, but they can also be used to screen 100 percent of the containers that enter U.S. ports. Using radiation portals is far more reliable way to prevent weapons of mass destruction from entering the United States than the labor intensive and somewhat unreliable method of targeting and physically inspecting only high risk containers. As Flynn and Wein noted, the integration of non-intrusive inspection devices into the supply chain could improve the trade off between cost and security due to "low equipment and labor cost of passive testing, the simplified logistics of testing at the gates, and the automated nature of passive testing."[19]

CBP plans to deploy portals at major points of entry including the twenty-two major seaports which handle ninety percent of inbound containerized cargo. According to agency officials, CBP has received the funding for portals at seaports, however this installation will be completed in March 2005 at the earliest. Currently, the Port of Norfolk is the only seaport in the nation with fully operational portal monitors at its major terminals. These portals were installed at the port's expense. The portals are located at various chokepoints ensuring every container which leaves the port by truck or train is screened for nuclear or radiological material.[20] Yet, according to port authority officials, the portals are integrated into daily operations and do not slow commerce.

SECURITY RECOMMENDATION

CBP should accelerate the installation of radiation detection portals and increase the number of VACIS machines at seaports to have an efficient and effective inspection process. DHS must begin to look at ways to better integrate the inspection process into supply chain operations. Efforts like those undertaken at the Port of Norfolk should be used as a model to determine ways to strengthen the inspection process without slowing the movement of goods. CBP should also invest in developing a device that combines the attributes of a radiation portal monitor and VACIS machine for the purpose of identifying a well hidden nuclear weapon in a cargo container.

In addition, VACIS machines should connect to an analysis center at which inspectors would review VACIS images and the images would be stored in a database. This center at would provide two benefits. First, it will allow VACIS images to be transmitted between ports, so if a container is screened at a CSI port overseas, the image could be sent to the domestic port where it contents could be re-examined. Second, an image database could also increase the effectiveness of VACIS inspections because inspectors would have files of images to reference.

- **Robust Inspections Require More Inspectors.**

Even as non-intrusive inspections are gradually integrated into port operations, CBP inspection programs will not be effective without significant personnel increases. Currently, DHS domestic and foreign container inspection operations do not have enough personnel to conduct vigorous cargo inspections. One such program is the Container Security Initiative (CSI). CSI sends inspectors overseas to inspect containers at the point of origin. DHS has reached agreements with 19 of the 20 "megaport" nations to allow CSI teams to operate. Megaports are the world's twenty largest ports by volume and handle roughly seventy percent of U.S.-bound cargo. CPB currently deploys five-person teams to CSI ports with the exception of some of the larger ports which have

[19] Lawrence Wein, Alex Wilkins, Manas Baveja, and Stephen Flynn, *Preventing the Importation of Illicit Nuclear Materials in Shipping Containers*. November 4, 2003.
[20] House Select Committee on Homeland Security staff trip to Norfolk, VA November 20, 2003.

two to three additional team members. The team consists of a research analyst, a special agent, and three inspectors. Currently 17 teams are fully operational.

While CSI is a very worthy effort, the current personnel levels are too low. Stephen Flynn has stated that CSI would require "the equivalent of a diplomatic service" to be an effective deterrent. One five person team deployed to a megaport is inadequate. The five-person team in Singapore, which sent more than 400,000 containers to the U.S. from March 2003 to January 2004, reviewed only sixty-three percent of cargo manifests.[21] This means 160,000 manifest were not even reviewed to determine the risk of the cargo. Additionally, the GAO has reported that under the CSI program inspectors are only temporarily stationed overseas for120 days.[22] Sending inspectors overseas for such a short period of time is not sufficient to ensure that they develop the relationships with foreign customs services necessary to obtain the information required to effectively target shipments. CBP has plans to expand CSI beyond the 20 megaports to cover 20 – 25 additional strategic ports around the world. However, under this plan, ports in high- risk countries such as Pakistan and Indonesia would not be covered. Moreover, the GAO has reported that CBP has no long term staffing plan to support the expansion of CSI to additional ports. The fiscal year 2005 budget includes funding to provide 98 additional CSI inspectors, however, given the expansion of CSI more resources may be needed to ensure cargo at foreign ports receive sufficient scrutiny before it is shipped to the U.S.

Inspection resources at U.S. ports are also stretched thin and will need to increase. According to a 2002 House Government Reform Committee report, the Port of New York/New Jersey had 64 inspectors dedicated to inspecting incoming cargo at a port which handles an average of one million inbound containers a year.[23] The report stated that the former Customs Service had 899 of its nearly 7,600 inspectors dedicated to seaports. To support CSI, CBP sends inspectors overseas for three to four months leaving U.S. ports short of inspectors. While ports have received additional inspectors, more will be needed to support the enhanced domestic and foreign inspection operations occurring since 9/11. For example, according to the GAO, CBP protocols call for random inspections of containers, even if they have not been identified as high-risk.[24] Before 9/11 inspectors would randomly examine containers to ensure the information on the manifest matched the contents of the container. However, CBP is not conducting random inspections at many ports because they only have enough inspectors to inspect only high risk cargo. This is the case in one major seaport, where random inspections have not been performed since 9/11 due to personnel constraints. [25]

---

[21] Weekly Statistics from CSI Singapore.

[22] [22] *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Criticial Success Factors* U.S. General Accounting Office, GAO-03-770. July 2003,12.

[23] *Federal Law Enforcement at The Borders and Ports of Entry* Report of the Subcommittee on Criminal Justice, Drug Policy and Human Resources, 80. July 2002.

[24] Richard Stanna, *Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers*. U.S. General Accounting Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. December 16, 2003, 11.

[25] Democratic Staff visit August 28-29, 2003.

SECURITY RECOMMENDATION

Customs and Border Protection should develop a human capital plan to determine the number of inspectors required to support CSI assignments of at least one year and increase cargo inspections at U.S. seaports.

Port Security

Seaports present terrorists with an attractive target because they are large, open facilities, readily accessible by water and land, often located in metropolitan areas, and interwoven with other transportation systems and critical infrastructure. The GAO has concluded that the large amount of high value cargo, hazardous materials, and people moving through ports at a given time make ports potential terrorist targets.[26] These factors led the FBI Assistant Director for Counterterrorism to state that ports are "inherently vulnerable" to terrorist attacks.[27] Similarly, Secretary of Homeland Security Tom Ridge stated that "The protection of our ports -- and the thousands of cargo containers that flow through them each day -- is a critical focus area of homeland security."[28] Congress acted to reduce ports vulnerability by passing the Maritime Transportation Security Act (MTSA) which President Bush signed on November 25, 2002.

SECURITY GAP: DHS Should Move Faster To Implement The Maritime Transportation Security Act.

The MTSA requires numerous measures designed to improve port security, including facility and vessel security plans, transportation identification cards, Coast Guard maritime security teams and vessel identification systems. While DHS has moved to implement certain provisions in the law, many important provisions have not been put into place. The Coast Guard has required ports and vessels to develop security plans, has brought seven Maritime Safety and Security Teams (MSST) online, and issued regulations requiring that vessels install identification systems. DHS has also begun to develop the Transportation Worker Identification Card (TWIC) with pilot projects in the ports of Philadelphia and Los Angeles/Long Beach.

However, DHS must begin to address other crucial MTSA sections such as the National Maritime Transportation Security Plan, foreign port security assessments, and a long range vessel tracking system.[29] The MTSA requires the Secretary of Homeland Security to prepare a national plan that coordinates the efforts at the federal level to prevent and respond to a terrorist attack at a port. The plan must include the assignment of responsibilities among federal agencies, and a surveillance system designed to ensure that threats to the maritime sector are identified and reported to appropriate federal and state agencies. The plan also requires that the flow of cargo through U.S. ports is reestablished as efficiently and quickly as possible in the event of a terrorist attack which would minimize the economic damage associated with an attack on a port. Additionally, the law requires the Secretary of Homeland Security to assess security at foreign

---

[26] *Port Security: Nation Faces Formidable Challenges in Making Initiatives Successful*. US General Accounting Office, JayEtta Z. Hacker, GAO-02-993T, August 5, 2003.
[27] Testimony of Gary Ball, Acting Assistant Director for Counterterrorism, Federal Bureau of Investigation before the Senate Judiciary Committee, January 27, 2004.
[28] Remarks on port security from Secretary Tom Ridge, June 12, 2003. www.dhs.gov
[29] Maritime Transportation Security Act, Sections 70103, 70108, and 70115.

ports and gives the Secretary the option of developing a long range vessel tracking system. This system would use satellite technology to track and monitor vessels to determine if they are threats and would give the Coast Guard the ability to intercept vessels before they reach an American port. At this time, there is no plan to re-route cargo in the event of a terrorist attack on a port, no plan on how the security at foreign ports will be assessed, or movement towards the development of a long range vessel tracking system.

SECURITY RECOMMENDATION

DHS should move faster to develop the National Maritime Transportation Security Plan to ensure coordination in the prevention and response to attacks or alerts and that economic damage is minimized by the efficient re-routing of cargo. DHS must also create a plan on how it will assess the security at foreign seaports and what the recourse will be if security gaps are discovered. If DHS wants to push its borders out to intercept threats to the U.S. before they arrive, it should develop a long range vessel tracking system to give the Coast Guard the ability to know the location of vessels well before they arrive in our territorial waters.

SECURITY GAP: Port Security Programs Are Underfunded.

In July 2003, in accordance with the MTSA, the Coast Guard issued port security regulations for ports, facilities, and vessels. The regulations require port facilities to hire security officers, and install barriers and surveillance systems, all of which were non-existent before 9/11. Unfortunately, the resources provided to our ports have not been sufficient to get the job done. The Coast Guard estimates that ports will spend $1.1 billion this year and $5.4 billion over ten years to comply with the regulations.[30] The only source of funding for security upgrades outside of port authorities' or facility owners' budgets is a port security grant in the DHS Office of Domestic Preparedness. Congress has taken the lead in supporting port security grants by appropriating $125 million in fiscal year 2004 bringing the total since 9/11 to $513 million. Despite Congress's support, funding for ports is still $566 million short of the Coast Guard's first year estimate. Yet, the Administration has only requested $46 million in its fiscal year 2005 budget for port security grants. In previous budgets, the Administration did not request any funding for port security.

Status of Port Security Grants

USCG 10-Year Estimate	USCG 1-Year Estimate	Appropriated Funds (FY 2002-04)	Admin. FY2005 Request	1st Year Funding Gap
$5.4 billion	$1.125 billion	$513 million	$46 million	**$566 million**

Ports have completed the assessments to determine what their vulnerabilities are and have developed security measures which will eliminate them. However, the lack of funding forces ports to purchase what they can afford instead what they actually need to increase security.

[30] *Federal Register* U.S. Coast Guard, Interim Final Rule Facility Security. July 1, 2003. p39319.

SECURITY RECOMMENDATION

Increasing grant funding will ensure ports can pay for adequate security measures which will aid in the prevention of terrorist attacks at America's seaports. While port security efforts require a public-private partnership, federal assistance must increase in order to ensure America's ports are secure without slowing economic activity. Many ports have diverted funding for infrastructure improvements designed to facilitate trade growth, to pay for security. To enable ports to make basic security improvements as quickly as possible, the federal government should fund the $566 million gap between estimated first year costs and the funds requested in the budget. To provide necessary funding in subsequent years DHS, port authorities, and industry should develop a cost sharing agreement.